Lab X1: Configuració estàtica de les NICs

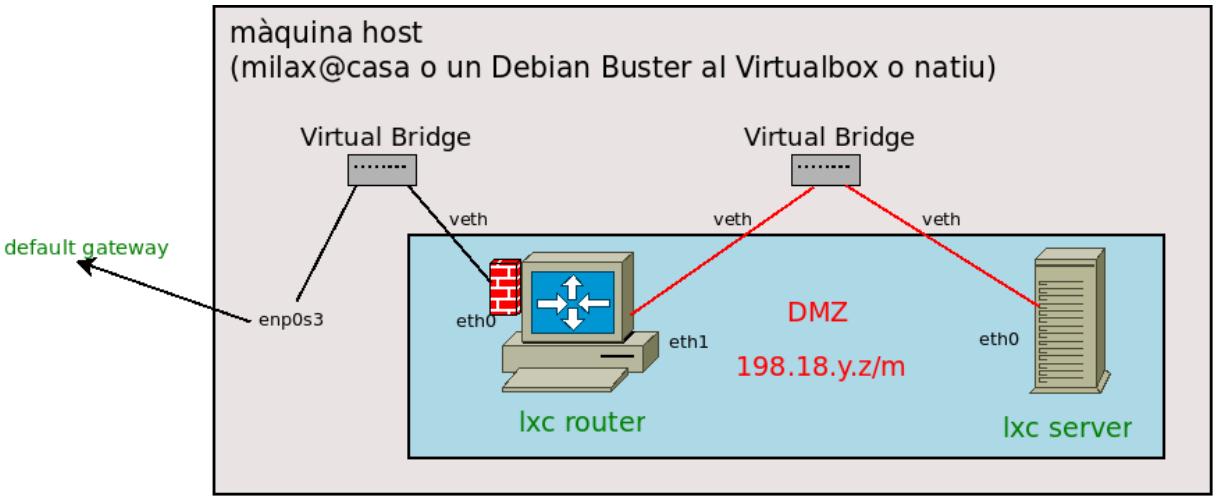
Objectius:

- Aplicar un esquema d'adreçament privat estàtic per a la nostra xarxa. Més endavant utilitzarem el protocol DHCP amb adreces dinàmiques. De moment tindrem una xarxa funcional.
- Fer les proves bàsiques per a comprovar la connectivitat és correcte.

Resum de les tasques a realitzar:

- Instal·larem la infraestructura de les màquines virtuals.
- Configurarem totes les interfícies amb IPs estàtiques.
- Activarem el servei ssh.
- Farem proves i guardarem els resultats.

Esquema de la topologia:



Usarem l'esquema d'adreçament assignat prèviament pel professor de forma personalitzada (el podreu trobar al moodle). Usarem les següents IPs:

classe C: **198.18.0.0/15** (Device Benchmark Testing) classe B: **172.24.0.0/16**

Per aquest laboratori sols usarem la classe C (DMZ).

1. Treball previ:

Necessitarem una màquina host amb un linux tipus **debian** (debian12, ubuntu>=20.04, mint, etc). Si no teniu un host/PC/portàtil amb linux, podreu usar el **virtualbox**.[1]

Heu de descarregar del moodle el fitxer **scripts_lxc_GSX24.tgz** i descomprimir-lo dins del debian, al directori de treball de les vostres pràctiques de GSX.

1 *llegiu l'annex del document inclòs al .tgz anomenat LLEGIU-ME.pdf.*

D'aquests scripts, utilitzeu **menu_GSXarxes.sh** per a crear els contenidors LXC[2] i la infraestructura de xarxa. Tarda bastant perquè usa **debootstrap** per a instal·lar el debian als contenidors (però sol cal a la primera execució).

La opció Start del menú obrirà automàticament **dos terminals** (un pel router i un altre pel servidor). Un cop fet el login (root,milax) ja podreu editar els scripts per automatitzar la configuració (usant els editors **vim** o **nano**).

Des del router hauríeu de tenir accés a Internet però no al server. Emperò, els dos tenen una IPv6 d'àmbit local que ens permetrà provar la seva connectivitat:

```
root@server:~# ip -6 address

root@router:~# ping -6 -I eth1 ff02::1              # Link-local multicast address
# o bé:
root@router:~# ping -6 -I eth1 fe80::XXXX:feff:etc  # la IPv6 del server
root@router:~# ip -6 neigh                          # per veure la taula de MACs
```

2. Enunciat:

Per a cada contenidor :
- creeu un directori de treball: mkdir /root/$HOSTNAME
- feu un *script* anomenat **labx1_static_config_$HOSTNAME.sh** que faci d'un sol cop les configuracions demanades als següents apartats:

A) Que configuri de forma estàtica les interfícies *ethernet*.

- Pel router (eth1) usarem el paquet **iproute2** per a implementar la configuració amb comandes ip a *l'script*. La IP que li assignareu serà la **primera disponible** (que és la menor del rang assignable).

- Al servidor (eth0) useu la el paquet **ifupdown** (amb la configuració al fitxer **/etc/network/interfaces**). La IP que li assignareu serà la **darrera disponible** (que és la major del rang assignable). Recordeu a posar la IP del router com a default gateway.

B) en el cas del router caldrà activar el ipv4 *forwarding* de forma permanent.

C) Com de moment no tenim servidor DNS, per a facilitar el treball, a cada màquina fareu que es posi el nom de l'altra màquina (router o server respectivament) i la seva IP al fitxer **/etc/hosts**.
Per a facilitar la extracció dels fitxers dels contenidors a la màquina amfitriona poseu també al seu /etc/hosts la IP externa del router. Exemple:

```
root@casa:~# ip=`lxc-info -Hi router | head -1` ; \
sed -i "s/^[^#]*router.*/$ip\trouter/" /etc/hosts
```

2 *De moment LXC ha de ser transparent. Ja ho veurem més endavant.*

D) Per a tenir sortida cap a Internet, al router cal canviar les IPs font (SA) privades per la IP externa del router (SNAT). Això ho farem amb la següent comanda de **iptables**:

```
# iptables -t nat -A POSTROUTING -s 198.18.b3.b4/m -o eth0 -j MASQUERADE
```

on:

-t nat:	usar la taula de nat (network address translation)
-A:	a la cadena de regles (*chain*) que s'aplica quan ja s'ha fet el *routing* (el SO ha cercat la IP destí (DA) a la taula d'encaminament).
-s	source IP: els datagrames que venen d'aquesta xarxa privada.
.net	el quart byte de la vostra adreça de xarxa
/m1	la màscara que se us ha assignat per a la DMZ
-o eth0:	sols pel tràfic que surt cap a Internet

Aquesta comanda només s'ha d'executar una vegada (per no allargar la cadena de regles innecessàriament): a *l'script* cal comprovar-ho.

E) Per a poder copiar fiters d'una màquina a una altra (o per a obrir una sessió) necessitarem tenir el **servei ssh** activat a cada màquina. Primer mostreu si s'està escoltant al seu port típic i mirem si està instal·lat. Per exemple:

```
grep ssh /etc/services
ss -4ltn                 # listennig tcp i numèric
dpkg -s openssh-server   # retorna $?=0 si està instal.lat
```

Si no està instal·lat, ho fem i ho comprovem:

```
sudo apt install -y openssh-server
sudo systemctl status ssh
ss -4lnt | grep ":22 "
```

L'usuari administrador (root) normalment té prohibit l'accés remot, però nosaltres ho activarem.
Poseu la següent línia al fitxer **/etc/ssh/sshd_config**:

```
PermitRootLogin    yes
```

i re-engegue el servei i el provem:

```
sudo systemctl restart ssh
ssh root@sever
```

Comproveu l'accés remot. Exemples:

```
milax@casa:~$ ssh router
root@router:~# ssh server
root@server:~/server# scp labx1_static_config_server.sh router:server/
```

Per extreu els directoris dels contenidors cap a l'amfitrió (útil per a 4. Final de sessió:):

```
milax@casa:~$ scp -r router:server/ .
milax@casa:~$ scp -r router:router/ .
```

3. Proves:

- Mostreu i analitzeu la configuració funcionant actualment (no la dels *scripts* o fitxers de configuració). Exemple:

```
ip -c address
ip -f inet address show eth1
```

- Mostreu i analitzeu la taula d'encaminament:

```
ip route
ip route get 8.8.8.8
```

- Feu **pings** d'una màquina a l'altre: s'haurien de respondre correctament.

```
root@server:~# pad=486f6c612047535820776f726c6421
root@server:~# ping -c5 -p $pad router
```

  - amb **tcpdump** podeu veure el contingut. Per exemple:

```
root@router:~#  tcpdump -nvX -i eth1 icmp | tee sortida_tcpdump.txt
```

on:

-n: format numèric (sense resoldre noms, ports etc)
-v: verbose, mostrant alguns camps del datagrama
-X: mostrant les dades en format hexadecimal i ASCII.
icmp: mostrar sols els paquets ICMP
(un altre exemple podria ser: 'icmp[icmptype] = icmp-echo')

- Feu pings des del **server** cap a l'exterior i des del host **amfitrió captureu** els paquets[3]:

```
sudo tcpdump -nvX -i lxcbr0 icmp | tee sortida_tcpdump_exterior.txt
```

Editeu el fitxer de sortida i observeu com s'ha aplicat la SNAT.

- Al router podeu comprovar les estadístiques de la SNAT:

```
root@router:~# iptables -t nat -nvL
```

3 *Per a posteriors pràctiques és important que recordeu que es pot capturar el tràfic dels ponts virtuals des de fora (del host amfitrió).*

4. Final de sessió:

- Executareu *l'script* proporcionat «**genera_sortida.sh**» a cada contenidor.
  Podeu mirar-lo: sols fa unes quantes comprovacions.
  Els dos fitxers generats els adjuntareu al lliurament del moodle.
  Important: deixeu-los tal com es generen, doncs s'usaran per a la avaluació.

- Guardeu tots els scripts i fitxers de sortida **en un únic tgz**[4] (de forma que es preservin els permisos).
  Aquest ha de contenir 2 directoris (pel router i pel server) i la sortida del tcpdump.
  Per exemple, al **amfitrió** haurem de fer:

```
sudo tar -cvzf labx1_$elsmeuscognoms.tgz router/ server/ sortida *.txt
```

- Copieu el tgz a un pendrive i/o al GoogleDrive/OneDrive/Dropbox etc.

- Trameteu a la tasca del moodle el .tgz (amb els directoris, els 2 *scripts* i les 3 sortida_*.txt).

Referències bàsiques:

- Transparències de teoria
- man pages:
  - ip: link, address, route , neigh
  - ifup, interfaces
  - hosts, ssh, sshd_config,
  - ping, tcpdump

4 *NO en un zip o rar o etc NI ho passeu NI ho editeu a cap altre sistema operatiu (ie: Windows), per a no perdre permisos, owner ni group, ni els final de línia.*